

# A novel identifiable data sharing mechanism for multiple participants in cloud computing

Jayalakshmi Karemallaiah, Prabha Revaiah

Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India

## Article Info

### Article history:

Received Sep 21, 2023

Revised Nov 7, 2023

Accepted Mar 16, 2024

### Keywords:

Cloud architecture

Cloud computing

Data sharing

Data storage

Security

## ABSTRACT

Recent applications and growth on the internet have generated a lot of popularity and adoption of cloud computing which aims to assure the various computing resources. Data storage is one of the primary resources offered by the cloud; however, considering the multiple users in the particular cloud raises major concerns due to security. Recent researches shown great potential for providing efficient data sharing with multiple users. However, tracing of the data provider is still concerned to be a major issue. Hence, this research work proposes identifiable data sharing for multiple users (IDSMU) mechanism which aims to provide security for multiple users in a particular cloud group. At first, IDSMU creates the general participants (GP)-key for secure access to data. Further, IDSMU creates the trusted participants (TP) based on the reputation which further helps in creating the key generation. A novel signature scheme is used for identifying the participants; IDSMU is evaluated on computation count and efficiency is proved by comparing with an existing model considering computation count.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Jayalakshmi Karemallaiah

Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology

Bangalore, India

Email: jayalakshmi\_112@rediffmail.com

## 1. INTRODUCTION

A branch of computing that is distributed is termed cloud computing. The application can be used or accessed irrespective of the place; the user tries to gain access, which is linked by their services. The technology consists of a number of shared resources that are provided on demand of the user as a service that is metered. The evolution of cloud computing is from the utility and grid application as well as services of computing [1]. The cloud has application models through which services are offered. The classification of these models are as follows: private, public, hybrid, and community cloud. The architecture of cloud computing is made up of two similar parts, one part consists of interactions with the client and the other part is used for the service providers of the cloud. The security as a service (SaaS) suggests that the data is encrypted by the user although the application models are a new invention in cloud computing. There is an absence of security in services of cloud computing models that compromises protection, which provides encryption as a source to users. There is delicate information that is present in the file, this information is encrypted within centralized servers or moved to the network for protection in relation to security problems [2], [3]. Hence, an emerging application for data security is initiated that prevents different threats relating to security issues to the information moved amidst the medium of communication using mechanisms of encryption. Figure 1 shows the major cloud security components such as compliance, production, access and identity, production, availability, response, and trust. Moreover, the designed cloud model should comply

with these components to be secure, distributed, and efficient data sharing especially when there are multiple participants involved.

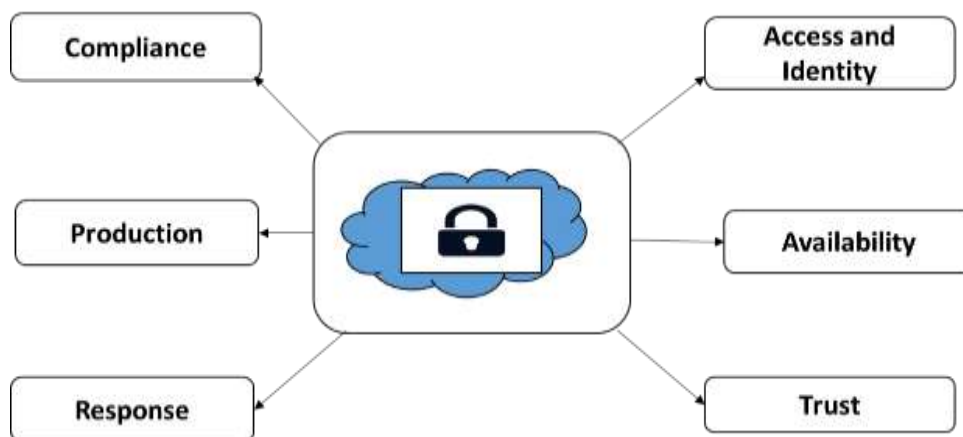


Figure 1. Cloud security component

Various constraints and problems occur with respect to the privacy and security of the data that is being sent within the medium that is open. The mechanisms for the security of this network are attractive as well as tough. Prior to the design of any algorithm or mechanism for security, the focus of the developer should lie on the possible attacks on the algorithm pertaining to security [4]–[7]. It is possible for each algorithm to oppose various attacks based on its properties as well as the algorithm that is selected about its requirement; the developer has to perform this big challenge. Eventually, constant monitoring is required for the protection of the data from these attacks. The attacks, which threaten the network, have been vastly categorized into passive attacks and active attacks. The attack is classified as an active attack if the resources of the system can be altered or its operations are affected. A passive attack is when the information is collected in opposition to obtaining the information accessed [8]–[10]. These attacks include breaking the site, service denial, usage of resources, deception of active attacks, breaching of data during traffic in the network, sniffing, collecting of information that is sensitive possessed by passive attacks. A huge count of researchers [11] has dedicated their attempts to propose schemes that are reliable for data searches that are secure within the cloud. Cloud computing has become a house-holding concept in technology, hence there has been many security and trust issues highlighted by various researchers. Some of the relevant research has been discussed here.

The researchers [12]–[15] has the process of cryptography that involves key generation is split into three classes. Initially, the service model of encryption that is based on support vector machine (SVM) for the generation of the key is from the encryption mode of operation that is conventional additional to few improvements. In order to complicate the process, the techniques of optimization are considered for the generation of the key in accordance with two various models of application that are used for computation for a cloud environment that is more secure [16]. In this paper, a scheme for data protection that is verified and searchable from an aided third party is proposed [17]. This uses the technology of cloud computing. To understand the protocol better, firstly, a system model that is user differentiated is introduced along with a structure for data storage that is cubic. Based on the structure of the data and system model, the integrity of the data that the users have downloaded or uploaded is reviewed at any given time and encrypted keywords are used to search the scholarly data online. In order to [18]–[20] aid the retrieval of efficient cipher text and keep up with the challenging performance, this paper proposes an encryption scheme that is lightweight attribute-based searchable encryption (LABSE), which recognizes the access control that is fine gained and the keyword search. During the reduction of the overhead for computation of the devices that are resource-constrained [21], [22]. The proposed work is an authentication user group that is content-centric to assure the accuracy and security of the data shared. The proposed authentication scheme for the group user uses the content of the user for the generation of the feature vector of the user. Moreover, the authentication scheme for the group that is based on every user's identity can assure the security of the network before the data is being shared. Additionally, the network operations that are regular remain unaffected and are not damaged due to the incidents that happen over the process of authentication [23].

The data involves text files that are plain, images of various sizes and formats as well as multimedia files. The transmission of data over the channel of communication without the main task being disclosed. Various mechanisms for security that include policies for access control, cryptography, digital signatures, and steganography are used in order to avoid the threats that are unauthorized. The most commonly used is cryptography for the protection of data. Furthermore, the contribution of this proposed work is as given below:

- This research work proposes identifiable data sharing for multiple users (IDSMU) mechanism, which aims for providing the multiple participants data-sharing model in the cloud.
- IDSMU creates general participants (GP)-key for secure access of data; further, with the help of a manager, it creates the trusted participant's (TP) group, and a later novel signature scheme is proposed to trace the identity of participants.
- IDSMU is evaluated considering the computation count; also, further evaluation is carried out by comparing with the existing model.

This particular research work is organized as follows: the first section starts with the background of cloud computing along with security concerns and architecture of the cloud. Further, the same section discusses the related work of existing models along with their shortcomings. The first section ends with research motivation and contribution of research work. The second section proposes IDSMU along with the proposed architecture, mathematical model, and algorithm. The third section evaluates the model by comparing it with the existing model.

## 2. PROPOSED METHOD

The protection of data or the privacy of data is an essential necessity for every paradigm relating to computing. Particularly, considering cloud computing, the data is operated and managed by a third party. Therefore, user data security could be breached for the archetype cloud computing. One such method for data protection with the cloud is through data encryption, which is made inarticulate.

### 2.1. System modelling

Figure 2 shows the system model of the proposed architecture; the general system model is designed based on user preference. For instance, a user with a similar domain tends to store the data in one particular data where the other members can have access. Moreover, these members are required to be genuine; this model tends to make the group data sharing not only efficient but also secure. In order to make it secure, the signature phenomena are utilized.

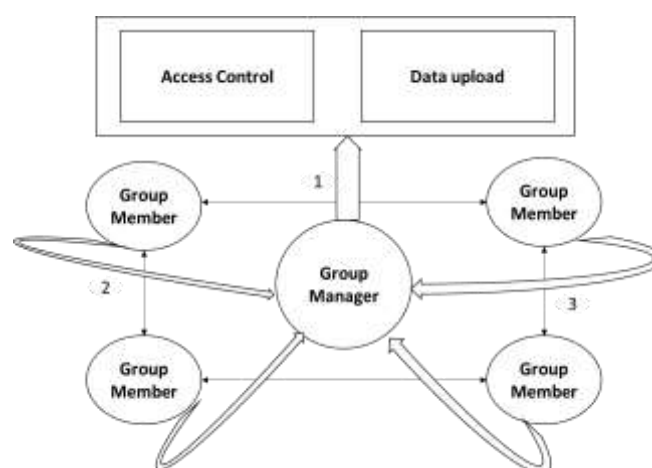


Figure 2. Proposed model

The proposed security model in Figure 2 comprises the three modules; the first module is a cloud that provides the users with unlimited storage. In addition, does not modify any data second module is the manager who is directly responsible for parameter generation of the designed model. The third module refers to the number of users based on the designed communication model. Further, there are three types of connection. Connection 1 indicates the registration and revocation, connection 2 is consensus development

among users to generate the key, and connection 3 is identifying the participants. In proposed model IDSMU mechanism, users register to the group manager for data sharing; the job of revocation is also carried out by the manager based on key generation.

**2.2. Client-Side modeling for key generation**

In client-side modeling, key is generated; IDSMU generates the key through two distinctive steps for participants. Key is generated based the on designed structure of  $(w, l + k, 1)$ ; this structure is designed according to the selection of prime number participants. However, considering the participants with a prime number might not be sufficient for the generation of keys as few messages might go missing. Thus, trusted members are created to support the data sharing along that also helps in creating the GP-key. TP selects the TP to create the key. TP are the one that has a good reputation in a particular group, it is denoted as  $m_q - m$ . In order to select the TP need to submit  $\varphi_j$  which indicates the identity to register with the manager to obtain the secret key  $(w_j, Z_j)$ . Once the registration and selection of TP are completed. Normal participants and TP require two steps to generate the GP. Further, the structure is designed for the  $o$  participants that need to share the data.

**2.2.1. Generation of participant’s signature**

Each participants chooses random number  $q_j$  as the secret key to compute  $L_j = d(H, q_j R_j)$  the that helps in generation of GP-key in particular group among the participants. Further, each participants member jadopts the algorithm of participants signature (PSign) for creating a signature on message with given secret key  $(Z_j, w_j)$ . Meanwhile participants receive message  $C_k = (L_k, \delta_k)$  from participants  $k$ . Further, key generation is parted into four scenario; in case of first scenario first participants requires receiving message from  $k$  participants. In case of second scenario, member participants require to receive message from participant’s  $k$  along with first participants. In case of third scenario, for participants  $j$ , it needs to receive the message from participant  $0$  and participants  $k$ . Remaining participants receives message from participants  $k$  and  $((j - 1)/l)$ . Algorithm 1 presents the algorithm for signature generation. Moreover, in order to design the algorithm few parameters need to be computed, these parameters are computed through (1) and (2).

$$\begin{aligned}
 S_1 &= \varpi \cdot T \\
 S_2 &= \varrho \cdot U \\
 S_3 &= Z_j + (\varpi + \varrho) \cdot G
 \end{aligned}
 \tag{1}$$

$$\begin{aligned}
 Q_1 &= s_\varpi \cdot T \\
 Q_2 &= s_\varrho \cdot U \\
 S_3 &= f(S_3, 0)^{s_w} \cdot f(G, V)^{-s_\varpi - s_\varrho} \cdot ff(G, V)^{-s_\varpi - s_\varrho} \\
 Q_4 &= s_w \cdot S_1 - \xi_1 \cdot T \\
 Q_5 &= s_w \cdot S_1 - \xi_1 \cdot T
 \end{aligned}
 \tag{2}$$

**Algorithm 1. Signature generation**

Input is given as a secret key  $(Z_j, w_j)$ ,  
 message and system parameters  
 Step1: Selection of random number

$$\varpi, \varrho, s_\varpi, s_\varrho, s_w, s_{\xi_1}, s_{\xi_2} \in Y_p'$$

Step2: Settings up numbers

$$\xi_1 = w_j \varpi, \xi_2 = w_j \varrho$$

Step3: Compute  $S_1, S_2, S_3, Q_1, Q_2, Q_3, Q_4, Q_5$   
 Step4: Generate hash value with

$$b = g_1(L, S_1, S_2, S_3, Q_1, Q_2, Q_3, Q_4, Q_5)$$

step5: compute  $q_\varpi, r_\varrho, r_w, r_{\xi_1}, r_{\xi_2}$   
 step6: Generation of group signature

$$\sigma = (T_1, T_2, T_3, C, s_a, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$$

Once each participant in a particular group receives the particular message, which further contributes to creating the GP-key from participants, a signature is verified with the message validity. After successful verification, each participant computes shows as per (3). Participants  $i$  receives message as  $D_k = \{B_{k,j}, \delta_k\}$  from other participants such that  $i \in E_j$  where  $B_{k,j}$  is for creating a particular group signature by participants  $j$  with algorithm 1. Each participant verifies the message validity, if verification is valid then the group key is computed through in the (4). Further, each participant in the group access the general participant's key that can be utilized for ensuring security in the cloud.

$$B_{k,j} = \prod_{w \in ED_k - \{j\}} L_w, \quad (w < m, j < m) \quad (3)$$

$$J = L_j(\prod_{w \in ED_k - \{j\}} B_{k,j}) \quad (4)$$

### 3. PERFORMANCE EVALUATION

The archetype cloud computing provides the resources as services to the users. This has different services that include database, platform, infrastructure, software, and protection. The main task of cloud computing is the data security of the cloud. It is widely classified as a data breach, authentication, and data protection. The data storage is either at the level of user or server and should be secure for access that is unauthorized. In order to evaluate the model, python is used as the programming language with system configuration of windows 10 packed with 16 GB random access memory (RAM) and 4 GB NVidea graphics. Further, a model is evaluated considering the client-side and server-side by varying the number of computation counts. In order to prove the model efficiency, the proposed model is compared with two baseline models [24], [25] and the existing model [26].

#### 3.1. Client-side evaluation

Figure 3 presents the client-side computation cost evaluation considering the time in seconds as the parameter. Moreover, in the case of client-side evaluation which can also be referred to as the key generation. Furthermore, evaluation is carried out with different computation counts. In the case of computation count 20, verifiable-scheme, novel-verifiable database (VDB) achieves the computation time of 0.4 seconds, 0.2 sec; secure-VDB achieves the large computational time with 0.4 seconds whereas the proposed model requires 0.0076 sec. Similarly, in the case of 40, 60, and 80, verifiable schemes require 0.3, 0.3, and 0.5 sec and novel-VDB requires 0.3, 0.3, and 0.5 seconds whereas secure-VDB requires 0.8, 1.25, and 1.5 seconds in a respective manner. However, in comparison of all these models, proposed IDSMU requires 0.0076, 0.00995, 0.009976, and 0.0099.

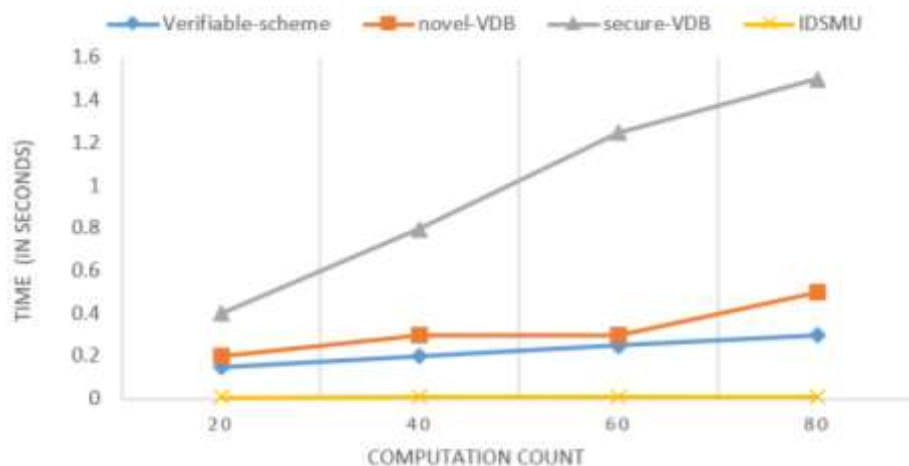


Figure 3. Client side evaluation

#### 3.2. Server-side evaluation

Figure 4 presents the server-side evaluation which is also known as the verification of key based on the computation count of 20, 40, 60, and 80. In case of computation count of 20, 40, 60, and 80, verifiable

scheme requires 0.45, 0.8, 1.35, and 1.75 respectively. Novel-VDB requires 0.15, 0.5, 0.75, and 1.25 respectively. Moreover, secure-VDB performs better on the server-side as it requires 0.15, 0.25, 0.52, and 0.55 sec respectively. However, in comparison with the existing and other models; IDSMU requires 0.006, 0.007, 0.008, and 0.0065 respectively.

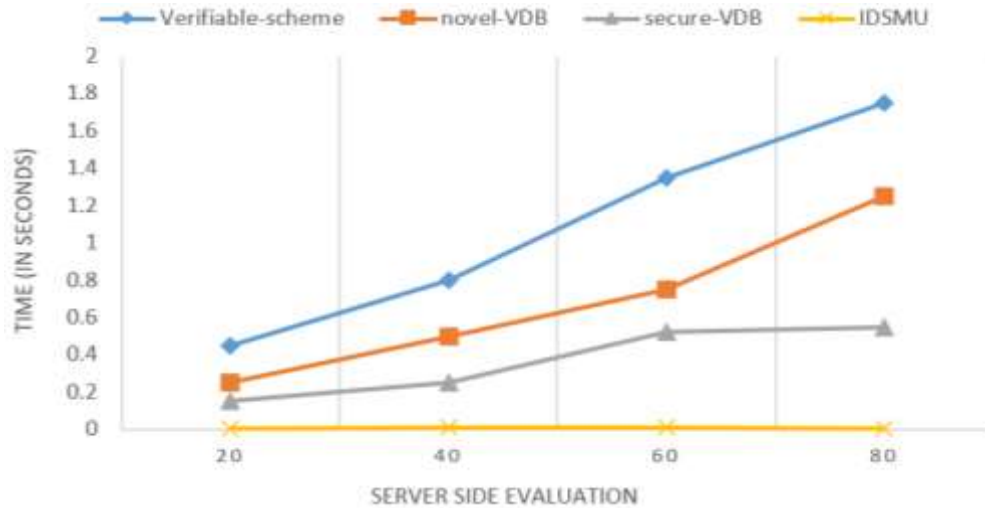


Figure 4. Server side evaluation

### 3.3. Comparative analysis and discussion

While sharing the data, security is a major concern, however efficient security is another major concern; efficient security deals with the optimal amount of time taken to perform the security part of it. In this section, a comparative analysis is carried out which shows the improvisation over the existing model which is depicted in Table 1. Comparative analysis is carried out based on the performance carried out on the client and server-side with the security aspect of key generation and key verification through varying the number of computations counts as 20, 40, 60, and 80.

Table 1. Improvisation over the existing model

Computation count	Client-side	Server-side
20	96%	95.4
40	96.83	96.92
60	96.67	98.44
80	96.66	98.81

On the client-side, it is observed that the existing model i.e., secure-VDB does not perform well and verifiable-scheme performs better. Hence, considering the comparison with verifiable scheme, IDSMU observes the improvisation of 96%, 96.83%, 96.67%, and 96.66% respectively for computation counts of 20, 40, 60, and 80. However, at the client-side secure-VDB performs better than the other existing model, thus comparative analysis is carried out with the secure-VDB. Hence, IDSMU observes 95.4% of improvisation in terms of 20-computation count, 96.92% in terms of 40-computation count, 98.44% of computation count in terms of 60-computation count, and 98.81% of improvisation in terms of 80 computation. Moreover, this improvisation has been observed in terms of seconds i.e., time taken to perform the key generation and key verification.

### 4. CONCLUSION





The security and privacy of data attain their more critical importance when a large number of organizations and enterprises use the open communication medium to transfer their messages. The confidentiality and integrity of the data must be guaranteed by the internet service providers in this scenario. This research work proposes an IDSMU mechanism that aims to assure secure data sharing considering the multiple participants in a particular cloud group. Moreover, IDSMU performs the novel signature-based

mechanism that can trace the identity of the data provider. IDSMU is proven to be a marginal improvement in comparison with another verifiable model; however, considering the vulnerability and complexity of the cloud model and increase in data, several other security analysis has to be carried out in the future.





## REFERENCE

- [1] M. Younis, W. Lalouani, N. Lasla, L. Emokpae, and M. Abdallah, "Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3746–3757, Sep. 2022, doi: 10.1109/JSYST.2021.3092519.
- [2] Y. Zhao, Y. Wang, X. Cheng, H. Chen, H. Yu, and Y. Ren, "RFAP: A revocable fine-grained access control mechanism for autonomous vehicle platoon," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9668–9679, Jul. 2022, doi: 10.1109/TITS.2021.3105458.
- [3] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving e-voting cloud system based on ID based encryption," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2399–2409, Jul. 2021, doi: 10.1007/s12083-020-00977-4.
- [4] F. Chen, Z. Li, C. Jiang, and J. Li, "Verifiable cloud data access: design, analysis, and implementation," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1135–1146, Mar. 2022, doi: 10.1109/JSYST.2020.3034105.
- [5] S. H. Sreedhara, V. Kumar, and S. Salma, "Efficient big data clustering using adhoc fuzzy c means and auto-encoder CNN," in *Lecture Notes in Networks and Systems*, vol. 563, 2023, pp. 353–368.
- [6] D. Samanta *et al.*, "Cipher block chaining support vector machine for secured decentralized cloud enabled intelligent IoT architecture," *IEEE Access*, vol. 9, pp. 98013–98025, 2021, doi: 10.1109/ACCESS.2021.3095297.
- [7] J. Shen, C. Wang, A. Wang, S. Ji, and Y. Zhang, "A searchable and verifiable data protection scheme for scholarly big data," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 1, pp. 216–225, Jan. 2021, doi: 10.1109/TETC.2018.2830368.
- [8] Y. Bao, W. Qiu, and X. Cheng, "Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2513–2526, Feb. 2022, doi: 10.1109/JIOT.2021.3063846.
- [9] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996–1010, Nov. 2019, doi: 10.1109/TDSC.2017.2725953.
- [10] K. Lee, "Comments on 'Secure data sharing in cloud computing using revocable-storage identity-based encryption,'" *IEEE Transactions on Cloud Computing*, vol. 8, no. 4, pp. 1299–1300, Oct. 2020, doi: 10.1109/TCC.2020.2973623.
- [11] I. Gupta, A. K. Singh, C. N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: a systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp. 71247–71277, 2022, doi: 10.1109/ACCESS.2022.3188110.
- [12] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 1136–1148, Oct. 2018, doi: 10.1109/TCC.2016.2545668.
- [13] Y. Tao, P. Xu, and H. Jin, "Secure data sharing and search for cloud-edge-collaborative storage," *IEEE Access*, vol. 8, pp. 15963–15972, 2020, doi: 10.1109/ACCESS.2019.2962600.
- [14] J. Sun, G. Xu, T. Zhang, H. Xiong, H. Li, and R. H. Deng, "Share your data carefree: an efficient, scalable and privacy-preserving data sharing service in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 822–838, Jan. 2023, doi: 10.1109/TCC.2021.3117998.
- [15] Q. Huang, Y. Yang, W. Yue, and Y. He, "Secure data group sharing and conditional dissemination with multi-owner in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1607–1618, Oct. 2021, doi: 10.1109/TCC.2019.2908163.
- [16] C. Lan, C. Wang, H. Li, and L. Liu, "Comments on 'attribute-based data sharing scheme revisited in cloud computing,'" *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2579–2580, 2021, doi: 10.1109/TIFS.2021.3058758.
- [17] J. Shen, H. Yang, P. Vijayakumar, and N. Kumar, "A privacy-preserving and untraceable group data sharing scheme in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2198–2210, Jul. 2022, doi: 10.1109/TDSC.2021.3050517.
- [18] X. J. Lin, L. Sun, and H. Qu, "Cryptanalysis of an anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2773–2775, 2021, doi: 10.1109/TIFS.2021.3065505.
- [19] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C. Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 344–357, Apr. 2018, doi: 10.1109/TCC.2017.2649685.
- [20] X. Li *et al.*, "A novel workflow-level data placement strategy for data-sharing scientific cloud workflows," *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 370–383, May 2019, doi: 10.1109/TSC.2016.2625247.
- [21] J. Cui, B. Li, H. Zhong, G. Min, Y. Xu, and L. Liu, "A practical and efficient bidirectional access control scheme for cloud-edge data sharing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 2, pp. 476–488, Feb. 2022, doi: 10.1109/TPDS.2021.3094126.
- [22] R. Mendes, T. Oliveira, V. Cogo, N. Neves, and A. Bessani, "Charon: a secure cloud-of-clouds system for storing and sharing big data," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1349–1361, Oct. 2021, doi: 10.1109/TCC.2019.2916856.
- [23] O. A. Khashan, "Secure outsourcing and sharing of cloud data using a user-side encrypted file system," *IEEE Access*, vol. 8, pp. 210855–210867, 2020, doi: 10.1109/ACCESS.2020.3039163.
- [24] J. Shen, A. Wang, C. Wang, J. Li, and Y. Zhang, "Content-centric group user authentication for secure social networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 3, pp. 833–844, Jul. 2020, doi: 10.1109/TETC.2017.2779163.
- [25] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation of computation over large datasets," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6841 LNCS, pp. 111–131, 2011.
- [26] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 546–556, Sep. 2015, doi: 10.1109/TDSC.2014.2366471.

**BIOGRAPHIES OF AUTHORS**

**Jayalakshmi Karemallaiah**     is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India. She has obtained Bachelors of Engineering BE degree in Computer Science and Engineering from Mysore University, Master's Degree M. Tech. Computer Network Engineering from VTU in 2009. And currently she is a research scholar at Dr. Ambedkar Institute of Technology doing her Ph.D. in Computer Science and Engineering. She has attended many workshops and induction programs conducted by various universities. Her areas of interest are cloud computing and computer networks. She can be contacted at this email: jayalakshmi\_112@rediffmail.com.



**Prabha Revaiah**     is currently working as a Professor in the Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India. She obtained her Bachelor of Engineering degree in Computer Science and Engineering branch from Mysore University. M.E in Computer Science and Engineering from Computer Science Department, UVCE, Bangalore University in the year 2003. She has 30 years of teaching experience. She was awarded Ph.D. in Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her research interest is in the area of wireless sensor networks and IoT. She can be contacted at this email: prabha.cs@drait.edu.in.